第 43 卷　第 1 期
2023 年 2 月
桂林电子科技大学学报
Journal of Guilin University of Electronic Technology
Vol. 43，No. 1
Feb. 2023

一种针对 AES 密码芯片的相关功耗分析方法

周　阳[1]，张海龙[2,3]，韦永壮[1,3]

（1. 桂林电子科技大学 广西密码学与信息安全重点实验室，广西 桂林　541004；
2. 中国科学院信息工程研究所 信息安全国家重点实验室，北京　100093；
3. 密码科学技术国家重点实验室，北京　100878）

摘　要：针对经典相关功耗分析过程中存在噪声等因素的影响，基于汉明重量与功耗轨迹之间存在线性相关的特性，提出一种针对 AES 密码芯片的相关功耗分析方法。根据密码算法 S 盒输出中间值汉明重量分布不均匀的特性，利用区分比将正确密钥与错误密钥进行筛选，得到与功耗轨迹相关性较强的一组明文。在密钥恢复阶段，通过观察这组明文输入找到前 2 个 S 盒的泄漏点后，利用分别猜测法逐一找出剩余 14 个 S 盒的泄漏区间，而无需遍历所有功耗轨迹即可捕获剩余字节的密钥信息。AT89S52 芯片实验分析表明，采用此方法仅需 9 条明文和对应功耗轨迹即可以 90％的成功率正确恢复出 AES 的单个字节密钥信息，计算复杂度仅为经典相关功耗分析的 4.1％，显著提升了相关功耗分析的效率。

关键词：相关功耗分析；密码芯片；汉明重量；S 盒

中图分类号：TN918.1　　**文献标志码**：A　　**文章编号**：1673-808X(2023)01-0041-07

A method of correlation power analysis for AES crypto chip

ZHOU Yang[1], ZHANG Hailong[2,3], WEI Yongzhuang[1,3]

(1. Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
3. State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: Aiming at the influence of the noise and other factors in the process of classical correlation power analysis, based on the linear correlation between Hamming weight and power traces, a correlation power analysis method for AES cryptographic chip is proposed. According to the uneven distribution of the median Hamming weight of the S-box output of the cryptographic algorithm, a set of plaintexts with strong correlation with the power traces is obtained by filtering the correct keys and the wrong keys by using the discrimination ratio. In the stage of key recovery, the leakage points of the first two S-boxes are found by observing this set of plaintext inputs, and the leakage intervals of the remaining 14 S-boxes are found one by one by using the separate guessing method, so that the key information of the remaining bytes can be captured without traversing all power traces. The experimental analysis of AT89S52 chip shows that the proposed method can correctly recover the one-byte key of AES with 90% success rate by using only 9 plaintexts and corresponding power traces, and the computational complexity is only 4.1% of the classical correlation power analysis, which significantly improves the efficiency of the correlation power analysis.

Key words: correlation power analysis; crypto chip; Hamming weight; S-box

收稿日期：2020-11-16
基金项目：广西重点研发计划(桂科 AB18281019)；广西密码学与信息安全重点实验室基金(GCIS201706)；桂林电子科技大学研究生科研创新计划(2018YJCX45)
通信作者：韦永壮（1976－），男，教授，博士，研究方向为信息安全。E-mail：walker_wyz@guet.edu.cn
引文格式：周阳，张海龙，韦永.壮一种针对 AES 密码芯片的相关功耗分析方法[J].桂林电子科技大学学报，2023，43(1)：41-47.

由比利时的 2 位密码学者 Joan Daemen 和 Vincen Rijmen 共同设计完成的高级加密标准 AES，采用典型的替代/置换结构，具有较高的安全性，较快的加解密速度及可便捷地在各种软件和硬件平台上使用等特点，目前已成为全球备受关注和广泛使用的分组密码之一。

侧信道技术利用密码算法在执行过程中泄露的物理信息来恢复密钥。如通过密码算法执行的能量消耗[1]、执行时间[2]、电磁信息[3]、声音[4]等直接获取密码算法的密钥，与传统密码分析相比，侧信道分析更具有实效性，对密码设备的正常运作产生了严重威胁。目前国内外主流的安全测评机构均把密码设备抵抗侧信道攻击的能力作为衡量其安全性的重要指标之一。

Kocher 等[1]利用简单能量分析（simple power analysis，简称 SPA）和差分能量分析（differential power analysis，简称 DPA）成功恢复出了 DES 算法的密钥信息。Brier 等[5]利用功耗能量分析（correlation power analysis，简称 CPA）成功恢复出 AES 算法的密钥信息。相关功耗分析通过利用密码设备泄露的物理信息与 S 盒输出中间值之间的统计学规律来分析密码设备密钥。该方法利用输出 S 盒的多比特信息建立模型恢复密钥，与 SPA 和 DPA 相比，相关功耗分析所利用的中间值信息更多，因而其攻击效果也比前 2 种方法更优。Kim 等[6]利用选择功耗轨迹的方法来恢复 DES 和 AES 的密钥。Hospodar 等[7]将机器学习用于侧信道分析。Heuser 等[8]将支持向量机（SVM）用于特征值的预处理工具和多比特汉明重量模型，以恢复 AES 的密钥信息，其恢复一个字节密钥需要大约 50 条功耗轨迹。文献[9]将神经网络用于侧信道分析，仅需一条功耗轨迹即可恢复出 AES 的密钥信息。Kim 等[10]提出一种通过原始数据的主成分分析来提高相关系数的分析方法。欧长海等[11]提出了一种基于汉明重量的放大模板攻击方法，大约需要 48 条功耗轨迹即可恢复出 AES 一个字节的密钥，有效提高了侧信道的攻击效率。Bartkewiz 等[12]引入了泄露原型学习的概念，并将其用于对 AES 的差分侧信道分析，通过每次 1 000 条功耗轨迹的平均进行学习求解，其攻击复杂度相对于传统侧信道分析仍较大。Picek 等[13]提出了一种用于侧信道分析的分层分类方法。Eloide 等[14]强调了互信息和成功率在侧信道分析中的重要性，但其在恢复密钥过程中的计算复杂度和存储复杂度仍较大。Ding 等[15]针对 AES 提出了一种基于遗传算法的多筛法侧信道分析方法，大约需要 280 条功耗轨迹可成功恢复出 AES 的密钥信息，与经典侧信道分析相比，其计算复杂度有了较大提高。近年来，许多学者借助机器学习对密码算法进行侧信道分析[16-19]。Bartkewiz 等[12]提出的攻击方法，在攻击前需将大量的功耗轨迹信息作为学习样本，在数据样本较少时无法正确恢复密钥信息，且其计算量仍较大。Ding 等[15]通过多种群遗传算法的相关功耗分析来解决传统遗传算法过早收敛的问题，但在离线恢复阶段所需计算量较大，在样本不足时易陷入局部最优解，使得攻击的成功率较低。如何减少相关功耗分析所需要的功耗轨迹数量，以提高攻击效率和成功率，是目前亟待解决的问题。

鉴于此，利用 S 盒输出中间值汉明重量分配不均匀的性质，将输出中间值分类后，选择区分较大的汉明重量与其对应明文的功耗轨迹来进行密钥恢复。在密钥恢复阶段，结合分别猜测法进行相关系数求解。与经典相关功耗分析相比，该方法能在仅需 9 条功耗轨迹条件下以 90%的成功率正确恢复出 AES 一个字节的密钥信息，计算复杂度仅为经典相关功耗分析的 4.1%。

1 密码算法 AES 与经典相关功耗分析的介绍

1.1 密码算法 AES 简介

高级加密标准 AES 分组的长度为 128 bit，其密钥的长度有 128、192 和 256 bit 三种。不同密钥长度所需迭代的轮数也不同：密钥长度为 128 bit 时，需迭代的轮数为 10 轮；密钥长度为 192 bit 时，需迭代的轮数为 12 轮；密钥长度为 256 bit 时，需迭代的轮数为 14 轮。128 bit 的中间状态可用一个状态矩阵表示，每个状态可看作一个 8 bit 的字节，则 16 个字节的编号为

$$\begin{pmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{pmatrix}。$$

除了在首轮运算前需要先进行轮密钥加操作，末轮无需进行列混合操作外，其他轮函数的操作均由字节替换（SB）、行移位（SR）、列混淆（MC）、密钥加法（KA）四种运算构成。

轮函数中唯一的非线性操作是字节替换，每个 S 盒由一个 8 bit 输入和 8 bit 输出的查找表组成，表示为 $y_{i,r}=S(x_{i,r})$，$i,r\in[0,3]$，其中：$y_{i,r}$ 为 S 盒的输出；$x_{i,r}$ 为 S 盒的输入；S 为 S 盒查表操作。

行移位变换将对字节替换后的每个状态循环移

位不同的位移大小。具体移位为

$$\begin{pmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{pmatrix} \xrightarrow{\text{行移位操作}} \begin{pmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{11} & x_{12} & x_{13} & x_{10} \\ x_{22} & x_{23} & x_{20} & x_{21} \\ x_{33} & x_{30} & x_{31} & x_{32} \end{pmatrix}$$

列混合变换是对中间状态矩阵中的每列进行操作，每个状态可视为有限域 GF(2^8)上的一个布尔表达式。

轮密钥加需将每个中间的状态 $x_{i,r}$ 与一个轮子密钥 $k_{i,r}$ 进行按位异或操作。

1.2　经典相关功耗分析流程

密码设备在执行加密或解密操作时产生的能量消耗 t 与密码算法的中间值 h 存在如下线性关系：

$$t = ah + b, \tag{1}$$

其中：h 为 S 盒输出中间值的汉明重量；a、b 为常数。

采用大量的功耗轨迹分析某时刻密码设备的能量消耗，并将能量消耗视为被处理中间值的函数，可分析出密码设备的密钥信息，具体步骤如下：

1)将密码算法的某个中间值 $y=(p,k)$作为攻击点，其中：p 为已知的明文；k 为待恢复的正确密钥。

2)采集密码设备的能量消耗：当密码设备正在运行时，利用示波器采集该设备对应的能量值消耗 t。

3)计算 h ：对于每个可能的候选密钥 k'_i，计算该候选密钥对应的 h。

4)利用汉明重量模型，计算 h 对应的能量消耗。

5)对于每个候选密钥 k'_i，计算 h 与功耗轨迹中所有采样点 t 之间的相关性系数，所得相关系数最大的密钥即为正确密钥。

相关功耗分析利用的统计学原理是：密码算法在设备中执行不同的操作时，消耗的能量也不同，若候选密钥是错误的，每条明文通过计算后所得对应的中间值是随机的，与对应功耗轨迹计算所得的相关系数很小；若候选密钥正确，则每条明文与对应正确密钥运算后所得的假设能量消耗与功耗轨迹一一对应，所得相关系数最大。利用该方法可正确恢复出密码设备的完整密钥信息。

相关性系数求解公式为

$$r_{i,j} = \frac{\sum_{p=1}^{n} (h_{p,i} - \overline{h_i})(t_{p,j} - \overline{t_j})}{\sqrt{\sum_{p=1}^{n} (h_{p,i} - \overline{h_i})^2 \sum_{p=1}^{n} (t_{p,j} - \overline{t_j})^2}}, \tag{2}$$

其中：P 为明文条数；$h_{p,i}$ 为第 P 条明文的第 i 个字节的假设能量消耗；$t_{p,j}$ 为第 P 条明文的第 j 列的真实能量消耗；$\overline{h_i}$、$\overline{t_j}$ 分别为列 h_i、t_j 的平均值；$r_{i,j}$ 为列 h_i 与 t_j 的线性关系，$i=1,2,\cdots,K$，$j=1,2,\cdots,T$。

在步骤 4)中，当采用汉明重量模型对每个字节密钥做假设能量消耗时，n 条明文与所有候选密钥通过异或运算后，经过 S 盒并计算其汉明重量。因汉明重量只有 9 种，相同的 n 条明文与不同的候选密钥 k'_i，$i\in(0,1,\cdots,K)$计算所得的汉明重量很大程度上是相同的，这对利用统计分析计算相关系数求解正确密钥有较大的噪声干扰。鉴于此，提出如下改进的相关功耗分析方法。

2　改进的相关功耗分析方法与功耗轨迹预处理

2.1　改进的相关功耗分析方法

性质 1　假设明文 P_i 的第 1 个字节为 $P_i^{(1)}$，而对应正确密钥 k 的第 1 个字节为 $k^{(1)}$，通过运算 $y=s(P_i^{(1)}\oplus k^{(1)})$可知，S 盒的输出中间值 y 的区分比是不同的，其中区分比表示在 $P_i^{(1)}$ 及其输出值汉明重量 $W_H(y)$固定时，所有满足 $y=s(P_i^{(1)}\oplus k^{*(1)})$的候选密钥 $k^{*(1)}$个数之和的倒数。

以 8 bit S 盒为例，明文 P_i 的第 1 个字节 $P_i^{(1)}$ 与正确密钥 k 的第 1 个字节 $k^{(1)}$经 S 盒运算后，输出值的汉明重量只有{0，1，2，3，4，5，6，7，8}九种，分别对应{1，8，28，35，70，35，28，8，1}九种候选密钥值。因此，$P_i^{(1)}$ 与正确密钥 $k^{(1)}$ 在密码设备中运算得到的汉明重量在 0 或 8 区间的区分比为 $R_{(0,8)}=1/1$；在 1 或 7 区间的区分比为 $R_{(1,7)}=1/8$；同理，$R_{(2,6)}=1/28$；$R_{(3,5)}=1/35$；$R_{(4)}=1/70$。

由以上分析可知，当正确密钥在汉明重量为 0 或 8 区域时，将正确密钥 $k^{(1)}$ 从候选密钥 $k^{*(1)}$ 中筛选出来的概率为 $R_{(0,8)}=1/1$；同理，$R_{(1,7)}=1/8$，$R_{(2,6)}=1/28$，$R_{(3,5)}=1/35$，$R_{(4)}=1/70$。因此，在相关功耗分析阶段，尽可能选择区分比大的明文与其对应的功耗轨迹进行密钥恢复，能够使正确密钥更容易从候选密钥中被筛选出。

以 AES-128 第 1 字节为例，说明采用区分比最小的明文与其对应功耗轨迹恢复密钥时的局限性。当输入相同明文与不同候选密钥并经过 S 盒运算后，得到的汉明重量如表 1 所示。

从表 1 可看出，对于猜测一个字节的密钥，$n'\in$ **N** 条明文已知且固定，功耗轨迹与明文一一对应且固定。当候选密钥为 0X11 时，上述 n' 条明文经过 S 盒操作，输出中间值的汉明重量为 4；当候选密钥为 0X17 时，n' 条明文经过 S 盒输出的汉明重量也为 4。其 2 列假设能量消耗 h 相同，用相同的汉明重量列向

量 $h'_{n'}$ 与相同的功耗轨迹列向量 t_j 计算相关系数，则无法判断正确密钥的唯一性。仅采用汉明重量为 4 的明文和功耗轨迹攻击结果如图 1 所示。

表 1 输入相同明文与不同候选密钥得到的汉明重量

输入的随机明文一个字节	候选密钥为 0X11 时所得汉明重量	候选密钥为 0X17 时所得汉明重量
0XDD	4	4
0X41	4	4
0X2C	4	4
0X22	4	4
⋮	⋮	⋮
0XD0	4	4

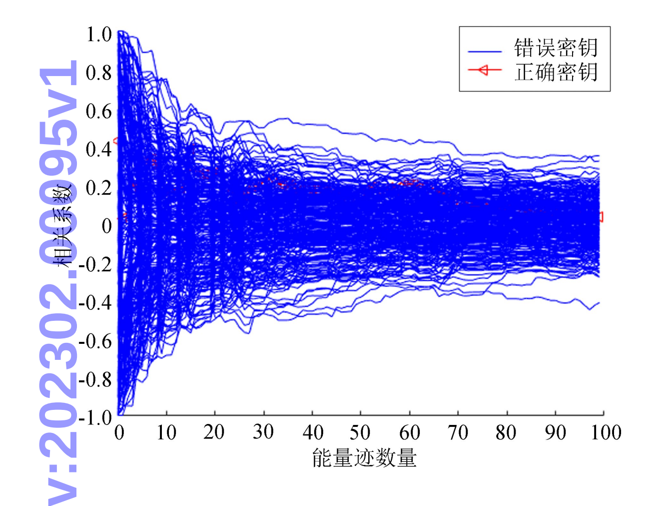


图 1 仅采用汉明重量为 4 的明文和功耗轨迹攻击结果

此外，明文每个字节的所有可能只有 256 种，当侧信道分析需要采集大量功耗轨迹时，会产生大量明文字节重复的可能性，其中经过 S 盒输出汉明重量为 4 的可能性最多，存在汉明重量分配不均匀的现象，这大大影响了相关系数的求解，进而影响相关功耗分析的效率。鉴于此，提出一种相关功耗分析方法，具体步骤如下：

1)将密码算法的某个中间值 $h=(p,k)$ 作为攻击点。

2)采集密码设备的能量消耗：当密码设备正在执行加密或解密时，利用示波器采集该设备对应的能量消耗。

3)计算 h：对于每个可能的候选密钥 k'_i，计算该候选密钥对应的 h。

4)计算 h 的假设能量消耗：对每个候选密钥 k'_i 计算经过 S 盒输出的汉明重量。将每个候选密钥 k'_i 输出的汉明重量为 0 和 8 的对应明文作为一类，汉明重量为 1 和 7 的对应明文作为一类，汉明重量为 4 的对应明文作为一类，以此类推。

5)对于每个候选密钥 k'_i，通过区分较大的明文与其对应功耗轨迹计算相关性系数，所得相关系数最大的密钥为正确密钥。

2.2 分别猜测法的功耗轨迹预处理

经上述明文选择后，采用经典相关功耗进行分析，通过计算所得的汉明重量矩阵与所采集的功耗轨迹的所有采样点来计算皮尔逊相关系数，从而恢复正确密钥。此过程计算量相当大，因为每条明文都需与候选密钥异或后，经 S 盒运算，再与采集的功耗轨迹的所有采样点来计算相关系数。这些采样点高达几千甚至几十万，大大影响了相关功耗分析的攻击效率。未经数据预处理的原始功耗轨迹如图 2 所示。

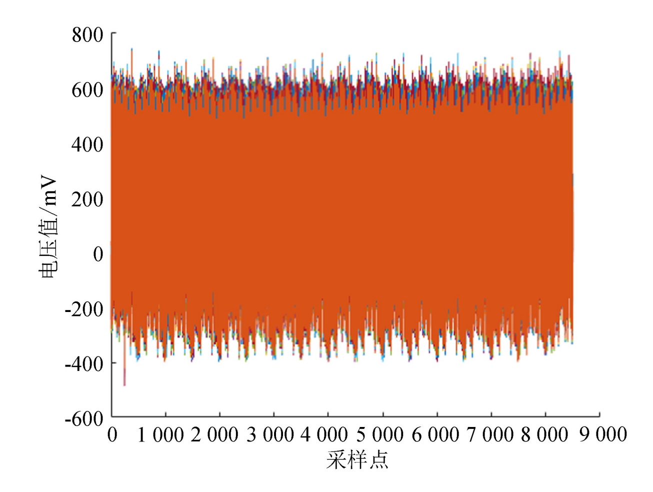


图 2 未经预处理的原始功耗轨迹

利用分别猜测法对功耗轨迹进行预处理，具体操作如下：

1)采用经典相关功耗分析，分别找到第 1、2 个 S 盒的泄漏点 D_1、D_2，如图 3、4 所示。将第 1 个泄漏点的位置到第 2 个泄漏点的距离记为 Δx，由于同一算法在同一台设备上执行相同操作，选择 AES-128 算法第 1 轮的每个 S 盒的输出作为攻击点，则其在执行该算法时整个功耗轨迹可看作一轮的 16 个 S 盒的全部泄露。

2)找到第 1、2 个 S 盒的泄露位置后，采用分别猜测法，通过泄漏点公式

$$D_n=D_1+(n-1)\Delta x,3\leqslant n\leqslant 16 \quad (6)$$

计算剩余 14 个 S 盒的泄漏点位置，而无需通过每次都遍历所有采集功耗轨迹的采样点来寻找泄漏点，从而恢复该字节的密钥。

3)找到映射后的对应泄漏点后，为提高实验的成功率，以该点为中心，左右 2 边各选取 5 个采样点，共 11 个采样点，组成一个泄露小区间，作为该 S 盒的泄

露区间，而无需再遍历所有采样区间，进而通过求相关系数来恢复密钥。

利用上述方法成功找到 AES 的 16 个 S 盒的泄漏点，如图 5 所示。

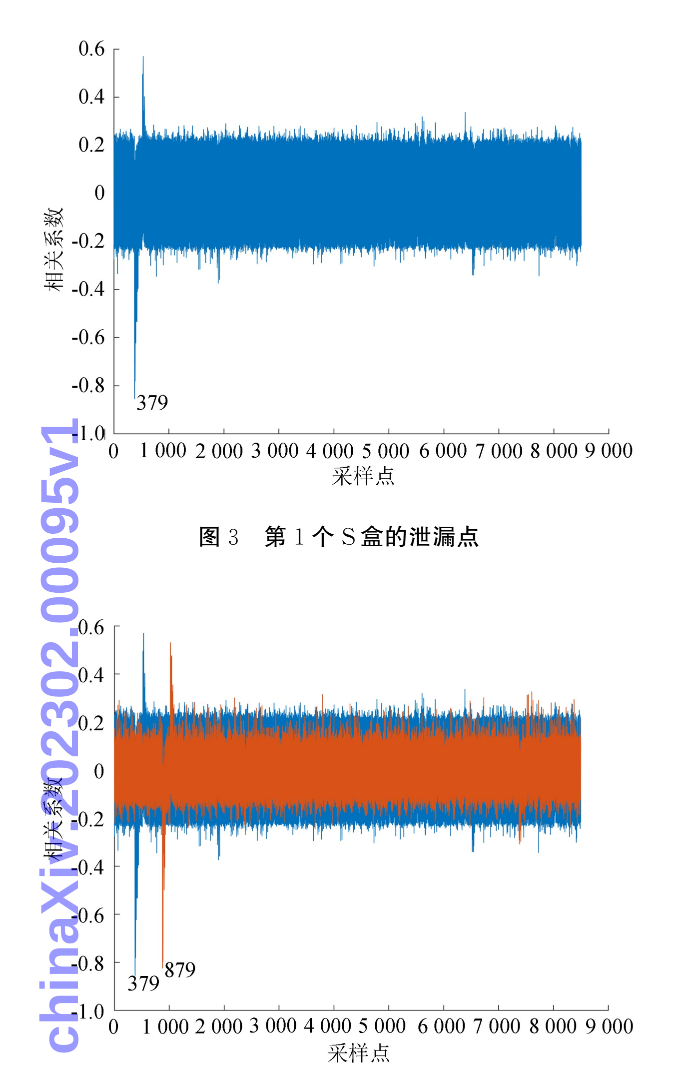


图 3　第 1 个 S 盒的泄漏点

图 4　第 1、2 个 S 盒的泄漏点

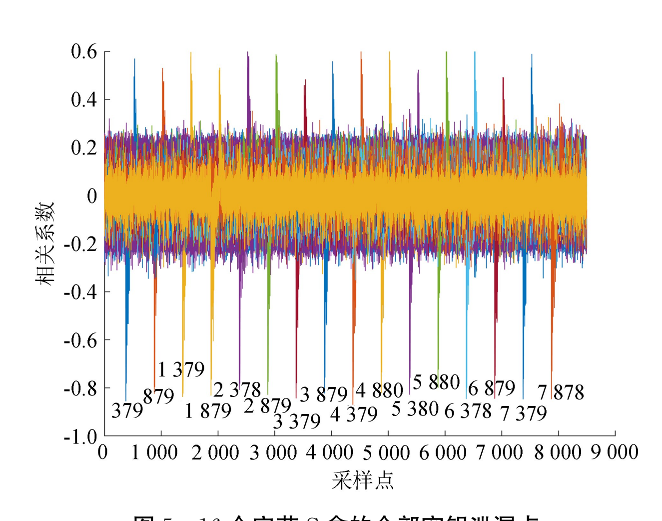


图 5　16 个字节 S 盒的全部密钥泄漏点

3　实验与分析

3.1　模拟实验

在 Windows 平台下，采用 C 语言对 AES 算法的功耗轨迹进行仿真实验。在仿真实验中，通过添加标准差分别为 $\sigma=3.0$ 和 $\sigma=5.0$ 的 2 种噪声来模拟 S-box 操作的功耗。在 2 种噪声情况下，使用相同的功耗轨迹，分别利用经典相关功耗分析和相关功耗分析方法来恢复密钥信息。功耗轨迹数从 10 增加到 1 000，间隔为 10，每组实验取 1 000 次实验的平均结果。忽略排序操作的计算代价，计算成本被估算为相关系数的平均计算次数，实验结果如图 6、7 所示。表 2 为在成功率分别为 50%、90%时，2 种方法所需要的功耗轨迹数和相应的计算量。

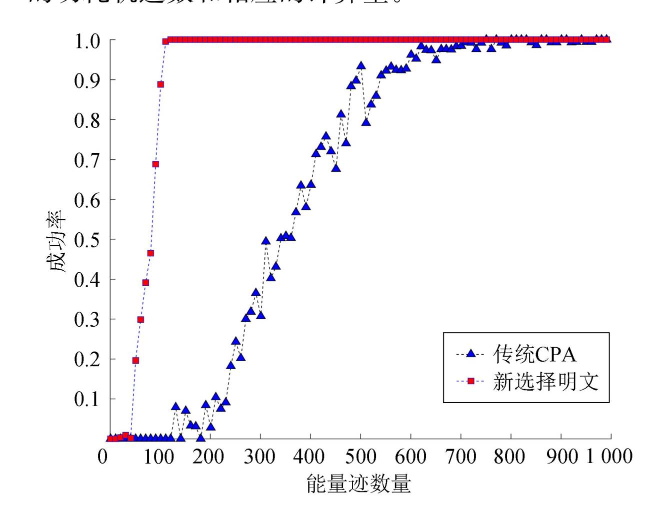


图 6　噪声为 $\sigma=3.0$ 时攻击效率

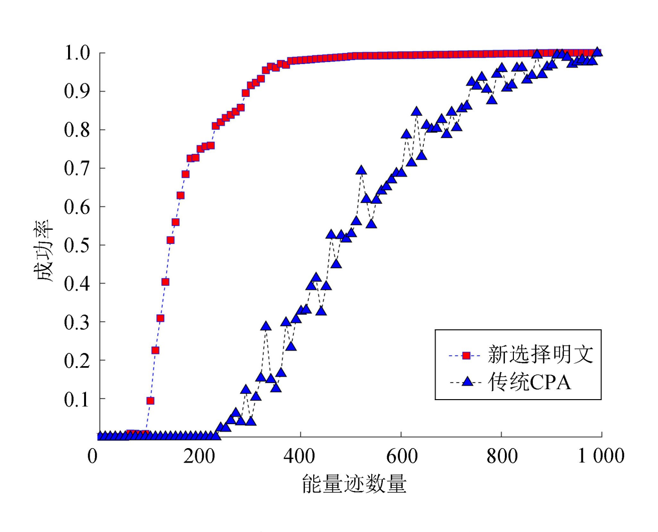


图 7　噪声为 $\sigma=5.0$ 时攻击效率

实验结果表明，当 $\sigma=3.0$ 时，相关功耗分析方法仅需 110 条功耗轨迹就可达到 90%的成功率，而经

表 2　不同噪声下成功率与功耗轨迹条数和计算量

攻击方案	成功率/%	σ=3.0		σ=5.0		正确 k 对应相关系数
		功耗轨迹	计算量	功耗轨迹	计算量	
文献[5]	50	350	1.147×10^{10}	470	1.541×10^{10}	0.56
本研究		95	3.930×10^{8}	150	6.203×10^{8}	0.63
文献[5]	90	510	1.671×10^{10}	750	2.458×10^{8}	0.67
本研究		110	4.594×10^{8}	310	1.282×10^{8}	0.78

典相关功耗分析则需要 510 条；当 $\sigma=5.0$ 时，相关功耗分析方法仅需 310 条功耗轨迹就可达到 90%的成功率，而经典相关功耗分析则需要 750 条，且相关功耗分析方法计算复杂度远低于经典相关功耗分析方法。本方案的另一个优点是正确密钥对应的相关系数更大，更有利于正确密钥的恢复。

3.2　单片机上的实验

真实功耗轨迹是在 AT89S52 单片机运行时采集而得，其时钟频率为 12 MHz，时钟每微秒震荡 12 个周期。选用 PICO Technology 示波器，采样频率为 1 GS/s。将 AES-128 算法烧入单片机，算法在执行“MOV A,@R0”时，利用间接寻址将 S-box 的输出值写入 A 寄存器，该 MOV 指令泄露了 S-box 输出值的汉明重量信息。

随机加密 100 个随机明文，并采集 100 条功耗轨迹。在进行恢复密钥时，对于每个可能的候选密钥，基于相关功耗分析方法，通过含有噪声较小的明文与其对应的功耗轨迹计算皮尔逊相关系数，仅需 9 条功耗轨迹就可正确恢复出 AES-128 算法第 1 轮第 1 字节的密钥 0X11，如图 8 所示，同理可恢复第 2 个字节密钥 0X22。在恢复剩余 14 个字节密钥时，采用分别猜测法，无需与采集功耗轨迹的所有采样点进行一一遍历，仅利用映射后的采样区间进行求解。在恢复第

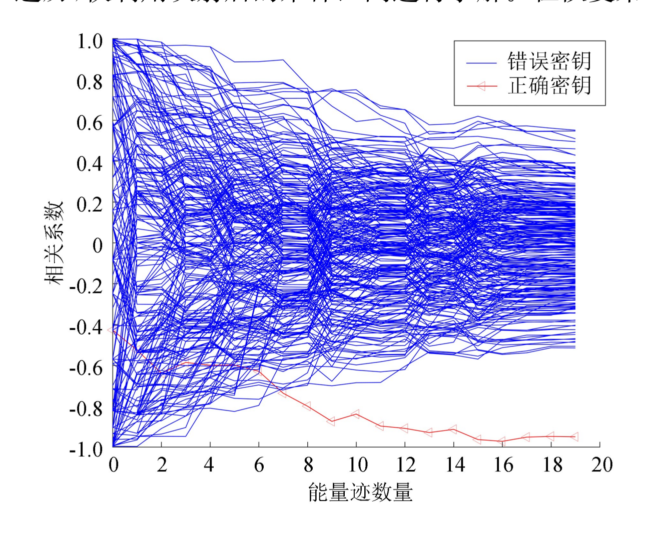


图 8　第 1 字节密钥相关系数与能量数量关系

1 个字节密钥时，对本方法与经典相关功耗分析方法做对比，结果如图 9 所示。本方法成功恢复出了 AES-128 第 1 轮的 16 个字节的正确密钥，如图 10 所示。

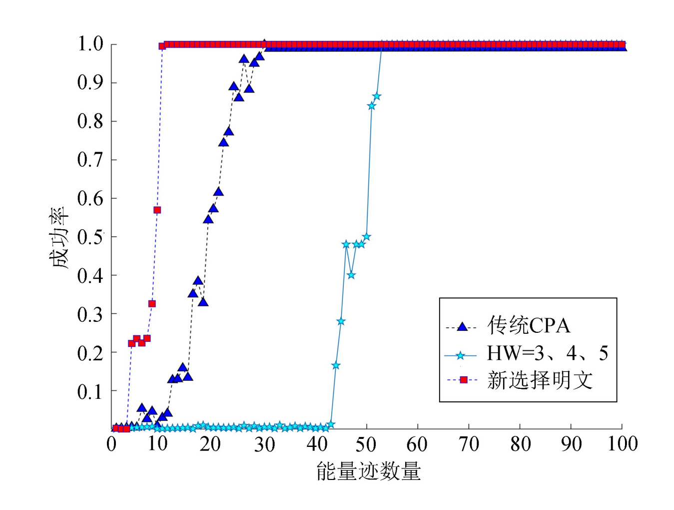


图 9　3 种攻击方案攻击效率

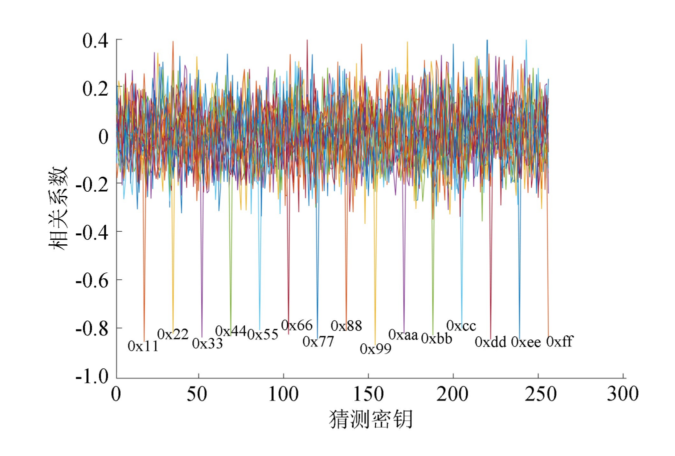


图 10　成功恢复出的 16 个字节密钥

真实环境下不同攻击方案的攻击效率如表 3 所示，真实功耗轨迹环境下恢复出的密钥与模拟环境下一致，表明本方法是有效的。当成功率相同时，本方法所需的功耗轨迹数更少，计算复杂度更低，正确密钥对应的相关系数更大，更有利于对其进行侧信道分析。

表 3　不同攻击方案的攻击效率

攻击方案	成功率/%	功耗轨迹数	计算量	正确 k 对应的相关系数
文献[5]	50	20	6.96×10^8	0.86
文献[6]		18	6.27×10^8	—
本研究		8	3.51×10^7	0.97
文献[5]	90	28	9.75×10^8	0.85
文献[6]		35	1.22×10^9	—
本研究		9	3.95×10^7	0.95

4　结束语

利用汉明重量模型，针对仅泄露汉明重量的密码芯片 AT89S52 提出了一种相关功耗分析方法。利用 S 盒输出中间值汉明重量分配不均匀的性质，将中间值的汉明重量进行分类。对每个候选密钥选择区分较大的一组汉明重量与其对应功耗轨迹，再结合分别猜测法对功耗轨迹进行预处理来恢复密钥信息。实验结果表明，通过本方法仅需 9 条功耗轨迹即可以 90% 的成功率恢复出 AES 一字节的密钥信息，其计算量仅为经典相关功耗分析的 4.1%。

参考文献：

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 1999: 388-397.

[2] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. Berlin, Heidelberg: Springer, 1996: 104-113.

[3] AGRAWAL D, ARCHAMBEAULT B, RAO J R, et al. The EM side-channel(s)[C]//International Workshopon Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2002: 29-45.

[4] SHAMIR A, TROMER E. A coustic crypt analysis[J]. Journal of Cryptology, 2017, 30(2): 392-443.

[5] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2004: 16-29.

[6] KIM Y, SUGAWARA T, HOMMA N, et al. Biasing power traces to improve correlation in power analysis attacks[C]//First International Workshop on Constructive Side Channel Analysis and Secure Design. Berlin, Heidelberg: Springer, 2010: 77-80.

[7] HOSPODAR G, MULDER E, GIERLICHS B, et al. Least squares support vector machines for side-channelanalysis[J]. Journal of Cryptographic Engineering, 2011, 1(4): 293-302.

[8] HEUSER A, ZOHNER M. Intelligent machine homicide[C]//International Workshop on Constructive Side-Channel Analysis and Secure Design. Berlin, Heidelberg: Springer, 2012: 249-264.

[9] MARTINASEK Z, ZEMAN V. Innovative method of the power analysis[J]. Radio Engineering, 2013, 22(2): 586-594.

[10] KIM Y, KO H. Using principal component analysis for practical biasing of power traces to improve power analysis attacks[C]//International Conference on Information Security and Cryptology. Cham: Springer, 2013: 109-120.

[11] 欧长海，王竹，黄伟庆，等. 基于汉明重量模型的密码芯片放大模板攻击[J]. 密码学报，2015，2(5)：477-486.

[12] BARTKEWITZ T. Leakage prototype learning for profiled differential side-channel cryptanalysis[J]. IEEE Transactions on Computers, 2015, 65(6): 1761-1774.

[13] PICEK S, HEUSER A, JOVIC A, et al. Climbing down the hierarchy: hierarchical classication for machine learning side-channel attacks[C]//International Conference on Cryptology in Africa. Berlin, Heidelberg: Springer, 2017: 61-78.

[14] DE CHÉRISEY E, GUILLEY S, RIOUL O, et al. Best information is most successful[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 1(4): 49-79.

[15] DING Yaoling, WANG An, YIU Siu-min. An intelligent multiple sieve method based on genetic algorithm and correlation power analysis[J]. IACR Cryptology ePrint Archive, 2019, 2019: 189.

[16] ZHANG Z, DING A A, FEI Y. A fast and accurate guessing entropy estimation algorithm for full key recovery[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 1(2): 26-48.

[17] NGUYEN P H, SAHOO D P. The interpose puf: secure puf design against state-of-the-art machine learning attacks[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 1(4): 243-290.

[18] ZAID G, BOSSUET L, HABRARD A, et al. Methodology for efficient CNN architectures in profiling attacks[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 1(1): 1-36.

[19] MASURE L, DUMAS C, PROUFF E, et al. A comprehensive study of deep learning for side-channel analysis[J]. Cryptographic Hardware and Embedded Systems, 2020(1): 348-375.

编辑：张所滨